AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1-9. (Canceled)

10. (Currently amended) ~~A unit according to claim 3,~~

An encryption/decryption unit for encrypting a plaintext into a ciphertext and/or decrypting a ciphertext into a plaintext, comprising:

first encryption/decryption means for performing an encryption or decryption process;

first substitution means for performing data substitution of an output from said first encryption/decryption means according to a predetermined permutation table;

second encryption/decryption means for performing an encryption or decryption process for an output from said first substitution means;

second substitution means for performing data substitution of an output from said second encryption/decryption means according to a predetermined permutation table;

third encryption/decryption means for performing an encryption or decryption process for an output from said second substitution means;

key generating means for generating intermediate keys respectively supplied to said first, second, and third encryption/decryption means and said first and second substitution means, and

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

said first and second substitution means functioning to perform identity conversion when the intermediate key generated by said key generating means contains predetermined data;

wherein said key generating means comprises:

dividing means for dividing key data K of a predetermined number of bits into a plurality of data and storing the divided data into respective registers;

expanded permutation means for reading out the divided key data from the respective registers and effecting an expanded permutation on the divided key data;

DES-SS key schedule means for generating intermediate keys K1 and K3 from a result of the expanded permutation performed by said expanded permutation means;

DES key schedule means for generating an intermediate key K2 from a result of the expanded permutation performed by said expanded permutation means; and

substitution schedule means for generating intermediate keys KK1 and KK2 from the contents of the registers.

11. (Original) A unit according to claim 10, wherein said expanded permutation means comprises an expanded permutation table for expanding input 56-bit key data into 64-bit data.

12. (Original) A unit according to claim 10, wherein said substitution schedule means receives one of the divided key data as a 32-bit key, and outputs an intermediate key KK1 input to said first substitution means and an intermediate key KK2 input to said second substitution means, said substitution schedule means comprising:

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

first means for directly outputting the input 32-bit key as an intermediate key KD1 of said first substitution means, calculating a logical OR of the intermediate key, and outputting the logical OR as an intermediate key KS1 (one bit) of said first substitution means; and

second means for shifting the input 32-bit key to the left to output the key as an intermediate key KD2 of said second substitution means, and calculating a logical OR of the intermediate key KD2 to output the key as an intermediate key KS2 (one bit) of said second substitution means.

a1

4 ~~13.~~ (Original) A unit according to claim ~~12~~ 3, wherein each of said first and second substitution means comprises an initial permutation section, an exclusive OR, a substitution portion, and an inverse permutation section, and said initial permutation section performs bit permutation of a 64-bit input and divides the permutation result into 8 blocks each comprising 8 bits,

32-bit data comprised of the first four 8-bit blocks of the output of said initial permutation section are directly input to said substitution portion, and 32-bit data comprised of the remaining four blocks is exclusive-ORed with the intermediate key KD, and a result of the exclusive-OR operation is output to said substitution portion,

said substitution portion outputs output data corresponding to an input using a permutation table when the 1-bit key KS is at "1", and outputs data identical to the input when the 1-bit key KS is at "0", and

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

 45

a

said inverse permutation section receives the output data from said substitution portion, performs bit permutation of the received data, and outputs the data as 64-bit data.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com